(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
28. November 2002 (28.11.2002)

PCT

(10) Internationale Veröffentlichungsnummer
WO 02/095637 A2

(51) Internationale Patentklassifikation[7]: G06F 17/60

(21) Internationales Aktenzeichen: PCT/DE02/01646

(22) Internationales Anmeldedatum:
7. Mai 2002 (07.05.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
101 25 017.7 22. Mai 2001 (22.05.2001) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **HAGN, Christine** [DE/DE]; Rosenweg 4, 85375 Neufahrn (DE). **MARKWITZ, Wernhard** [DE/DE]; Reichenbachstr. 25, 80469 München (DE). **KAIJSER, Per** [SE/DE]; Moarstr. 18, 85737 Ismaning (DE).

(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, 80506 München (DE).

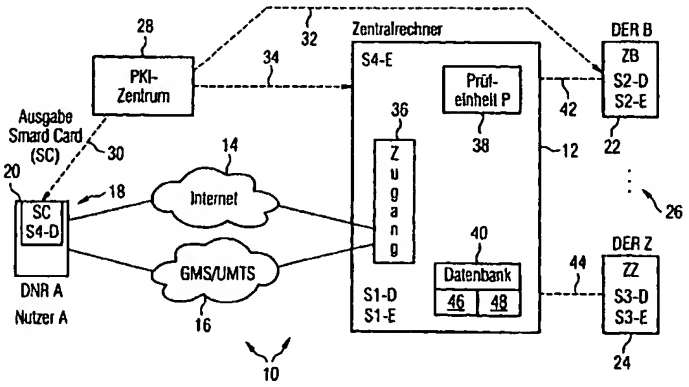
(81) Bestimmungsstaat *(national)*: US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR PROVIDING SERVICES IN A DATA TRANSMISSION NETWORK AND ASSOCIATED COMPONENTS

(54) Bezeichnung: VERFAHREN ZUM ERBRINGEN VON DIENSTEN IN EINEM DATENÜBERTRAGUNGSNETZ UND ZUGEHÖRIGE KOMPONENTEN



32.. CENTRAL COMPUTER
28.. PUBLIC KEY INFRASTRUCTURE (PKI) CENTER
30.. OUTPUT SMART CARD (SC)
14.. INTERNET
NUTZER A = USER A
38.. TEST UNIT P
40.. DATABASE
36.. ACCESS

(57) Abstract: The invention relates to, among other things, a method according to which an access function (36) for a number of service user computers (18) permits a connection between the service user computer (18) and a service provider computer (22 to 26), which is selected by a service user (A), according to requests submitted by a service user computer (18). The insertion of an access function (36), and the use of a test unit (38) make it possible to secure useful data that is to be processed in a reliant manner.

[Fortsetzung auf der nächsten Seite]

WO 02/095637 A2

Erklärungen gemäß Regel 4.17:

— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR)*

— *Erfindererklärung (Regel 4.17 Ziffer iv) nur für US*

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Erläutert wird unter anderem ein Verfahren, bei dem eine Zugangsfunktion (36) für mehrere Dienstnutzungsrechner (18) abhängig von Anforderungen von der Seite eines Dienstnutzungsrechners (18) eine Verbindung zwischen dem Dienstnutzungsrechner (18) und einem durch einen Dienstnutzer (A) ausgewählten Diensterbringungsrechner (22 bis 26) ermöglicht. Das Zwischenschalten einer Zugangsfunktion (36) und das Verwenden einer Prüfeinheit (38) ermöglicht die Sicherung von vertrauensvoll zu behandelnden Nutzdaten.

Beschreibung

Verfahren zum Erbringen von Diensten in einem Datenübertragungsnetz und zugehörige Komponenten

Die Erfindung betrifft ein Verfahren, bei dem eine Zugangsfunktion für mehrere Dienstnutzungsrechner eine Verbindung zwischen dem Dienstnutzungsrechner und einem Diensterbringungsrechner ermöglicht.

So lässt sich mit Hilfe der Zugangsfunktion die Internetseite eines Unternehmens aufrufen, das seine Dienstleistungen über das Internet verkauft. Die Zugangsfunktion prüft unter anderem die Identität des Dienstnutzers, beispielsweise durch Abfrage eines Passwortes.

Bisher war es üblich, dass jedes Unternehmen seine eigene Zugangsfunktion hatte und dass die Kundendaten von jedem Unternehmen einzeln und damit unter Umständen mehrfach gespeichert worden sind. Die Sicherheit der Kundendaten ist bei einer solchen verteilten Speicherung der Kundendaten nur eingeschränkt gewährleistet. Aufgrund dieser Einschränkungen der Sicherheit entwickelte sich ein Handel mit Kundendaten. Durch einen solchen Handel sinkt die Akzeptanz der Diensterbringungsverfahren über das Internet erheblich, insbesondere wenn Kundendaten gehandelt werden, die im Zusammenhang mit der Kaufkraft, dem Kreditrahmen oder anderen finanziellen Daten der Kunden stehen.

Es ist Aufgabe der Erfindung, zum Erbringen von Diensten in einem Datenübertragungsnetz ein einfaches Verfahren anzugeben, das es insbesondere gestattet, Kundendaten vor Missbrauch besser zu schützen als bisher. Außerdem sollen ein zugehöriges Programm und eine zugehörige Datenverarbeitungsanlage angegeben werden.

Die auf das Verfahren bezogene Aufgabe wird durch die im Patentanspruch 1 angegebenen Verfahrensschritte gelöst. Weiterbildungen sind in den Unteransprüchen angegeben.

Die Erfindung geht von der Überlegung aus, dass zum Sichern der Kundendaten ein erheblicher Aufwand erforderlich ist, der die Akzeptanz der Erbringung von Diensten über das Internet auf der Seite der Dienstanbieter senken würde. Um dem aber entgegenzuwirken, wird beim erfindungsgemäßen Verfahren eine Zugangsfunktion verwendet, die eine Verbindung zwischen einem Dienstnutzungsrechner und einem von mehreren durch einen Dienstnutzer auswählbaren Diensterbringungsrechner ermöglicht. Außerdem wird eine zentrale Datenbank eingerichtet, in der für die verschiedenen Dienstnutzer zu sichernde Nutzerdaten gespeichert werden, die zur Erbringung der Dienste verschiedener Diensterbringungsrechner erforderlich sind. Durch diese Zentralisierung der Zugangsfunktion und der Datenbank lässt sich der Aufwand für die Sicherung der Kundendaten auf eine Vielzahl verschiedener Diensterbringer verteilen. Die Akzeptanz auf der Seite der Diensterbringer steigt also.

Durch das Verwenden der zentralen Datenbank kann auch den Dienstnutzern zugesichert werden, dass ihre Daten vor Missbrauch geschützt sind. Somit erhöht sich die Akzeptanz von Verfahren zur Diensterbringung über ein Datenübertragungsnetz auch auf der Seite der Dienstnutzer.

Das erfindungsgemäße Verfahren geht außerdem von der Überlegung aus, dass die zu sichernden Kundendaten zwar im Rahmen der Diensterbringung erforderlich sind, jedoch nicht unbedingt dem Diensterbringer übergeben werden müssen. Deshalb wird beim erfindungsgemäßen Verfahren nach der Verbindungsaufnahme zwischen einem Dienstnutzungsrechner und einem ausgewählten Diensterbringungsrechner im Rahmen der Diensterbringung für den den Dienstnutzungsrechner nutzenden Dienstnutzer an eine zentrale Prüfeinheit eine Anforderung gestellt. Diese Anforderung betrifft beispielsweise die Zusi-

cherung der Zahlungsfähigkeit des Dienstnutzers. Die Anforderung kann nur unter Zugriff auf zu sichernde Nutzerdaten des Dienstnutzers bearbeitet werden. So sind beispielsweise Deckungszusagen einer Bank für spätere Nachweiszwecke zu speichern. Andererseits wird aber auch eine frühere Deckungszusage gelesen, falls sie noch gültig ist. Eine Prüfeinheit, die unabhängig von den Diensterbringungsrechnern arbeitet, bearbeitet die Anforderung unter Zugriff auf zu sichernden Nutzerdaten des Dienstnutzers. Nur das Bearbeitungsergebnis nicht aber ein zu sicherndes Nutzerdatum selbst wird von der Prüfeinheit an den die Anforderung stellenden Diensterbringungsrechner übermittelt. Der betreffende Diensterbringungsrechner erbringt dann seinen Dienst abhängig vom Bearbeitungsergebnis. Durch diese Maßnahme wird also erreicht, dass die zu sichernden Kundendaten selbst nicht an einen Diensterbringungsrechner übermittelt werden müssen. Nur die Prüfeinheit hat Zugriff auf die zu sichernden Daten. Damit ist ein Handel mit den zu sichernden Kundendaten erschwert und einem Missbrauch wird wirksam vorgebeugt.

Bei einer Weiterbildung des erfindungsgemäßen Verfahrens gehören die Diensterbringungsrechner verschiedenen Betreibern. Nach der Anwahl eines Diensterbringungsrechners wird dessen Berechtigung zum Stellen von Anforderungen mit Hilfe eines Berechtigungsprüfverfahrens geprüft. Das Bearbeitungsergebnis wird nur bei bestehender Berechtigung von der Prüfeinheit an den Diensterbringungsrechner übermittelt. Bei fehlender Berechtigung wird kein Bearbeitungsergebnis übermittelt. Bei fehlender Berechtigung muss die Anforderung nicht bearbeitet werden. Durch das Prüfen der Berechtigung zur Seite der Diensterbringungsrechner hin lässt sich gewährleisten, dass keine Anforderungen durch Unberechtigte gestellt werden, welche die Bearbeitungsergebnisse dann missbräuchlich verwenden könnten.

Bei einer anderen Weiterbildung des erfindungsgemäßen Verfahrens werden die zu sichernden Nutzerdaten verschlüsselt ge-

speichert. Die Diensterbringungsrechner haben keinen Zugang zu einem zum Entschlüsseln erforderlichen digitalen Schlüssel. Das Verschlüsselungsverfahren bzw. ein zu verwendender Schlüssel lässt sich mit Hilfe konstruktiver und/oder elektronischer Sicherungsmaßnahmen geheimhalten. Selbst wenn die zu sichernden Kundendaten durch Unbefugte kopiert werden, sind diese nicht im Besitz des zum Entschlüsseln erforderlichen Schlüssels. Damit bleiben die zu sichernden Daten trotz des unberechtigten Kopierens vor Missbrauch geschützt.

Bei einem zweiten Aspekt der Erfindung, der auch als eine nächsten Weiterbildung des erfindungsgemäßen Verfahrens nach dem zuvor erläuterten Aspekt der Erfindung auftritt, sind in einer Datenbank Dienst-Nutzerdaten gespeichert, die dienstbezogene Daten für die Dienstnutzer einzelner Diensterbringungsrechner enthalten. Nach der Anwahl eines Diensterbringungsrechners wird dessen Berechtigung zum Empfangen von Dienst-Nutzerdaten betreffend den durch ihn erbrachten Dienst geprüft. An den ausgewählten Diensterbringungsrechner werden die angeforderten Dienst-Nutzerdaten nur bei bestehender Berechtigung übermittelt. Übermittelt werden immer nur die dienstbezogenen Daten desjenigen Dienstnutzers, der den ausgewählten Diensterbringungsrechner ausgewählt hat. Der Diensterbringungsrechner erbringt dann seinen Dienst unter Verwendung der übermittelten Dienst-Nutzerdaten. Durch die Prüfung der Berechtigung zum Empfangen von Dienst-Nutzerdaten lässt sich gewährleisten, dass die Dienst-Nutzerdaten einzelner Diensterbringer nicht missbräuchlich an Dritte übermittelt werden.

Bei einer Ausgestaltung ist die Datenbank zum Speichern der Dienst-Nutzerdaten Bestandteil der zentralen Datenbank. Bei einer anderen Ausgestaltung wird zum Prüfen der Berechtigung für das Stellen von Anforderungen und zum Prüfen der Berechtigung für das Empfangen von dienstbezogenen Dienst-Nutzerdaten dasselbe Prüfverfahren ausgeführt. Somit ist jeweils nur ein Berechtigungsprüfverfahren auszuführen.

Bei einer Weiterbildung des Verfahrens mit einer Datenbank für Dienst-Nutzerdaten sind die Dienst-Nutzerdaten verschlüsselt gespeichert und werden auch verschlüsselt übertragen. Verschiedene Diensterbringungsrechner verwenden verschiedene digitale Schlüssel zum Entschlüsseln der Dienst-Nutzerdaten. Durch diese Maßnahme wird gewährleistet, dass die Dienst-Nutzerdaten nur durch den berechtigten Diensterbringer entschlüsselt werden können. Andere Diensterbringungsrechner und auch der Betreiber der Datenbanken sind nicht in der Lage, die Dienst-Nutzerdaten zu entschlüsseln. Damit lassen sich die Dienst-Nutzerdaten wirksam vor Missbrauch schützen. Die Speicherung der Dienst-Nutzerdaten außerhalb des den Dienst erbringenden Unternehmens wird so leichter akzeptiert.

Bei einer weiteren Ausgestaltung des Verfahrens mit Verwendung von Dienst-Nutzerdaten sind die Dienst-Nutzerdaten zusätzlich oder alternativ mit einem zentralen Verschlüsselungsverfahren verschlüsselt. Zum Entschlüsseln der mit dem zentralen Verschlüsselungsverfahren verschlüsselten Nutzdaten wird ein digitaler Schlüssel verwendet, zu dem die Diensterbringungsrechner keinen Zugang haben. Durch diese Maßnahme lassen sich sowohl von den Diensterbringungsrechnern kommende unverschlüsselte Daten als auch verschlüsselte Daten nach dem gleichen zentralen Verfahren sicher speichern. Eine doppelte Verschlüsselung bietet außerdem eine zusätzliche Sicherheit gegen den Missbrauch der dienstbezogenen Daten.

Bei einer anderen Weiterbildung des erfindungsgemäßen Verfahrens werden in einer von mehreren Diensterbringungsrechnern genutzten Datenbank digitale Daten über Zahlungsvorgänge für verschiedene Diensterbringungsrechner gespeichert. Diese Datenbank ist beispielsweise Bestandteil der zentralen Datenbank. Es lassen sich die oben genannten Verschlüsselungsverfahren auch zum Sichern der Daten über die Zahlungsvorgänge einsetzen. Außerdem wird eine Berechtigungsprüfung vor der Übermittlung der Daten über die Zahlungsvorgänge ausgeführt.

Bei einer weiteren Weiterbildung des erfindungsgemäßen Verfahrens wird die Berechtigung des Dienstnutzers unter Verwendung eines Berechtigungsprüfverfahrens geprüft. Die Auswahl wird nur beim Vorliegen einer Berechtigung zugelassen. Durch diese Berechtigungsprüfung lässt sich ein Missbrauch von der Seite der Dienstnutzer her verhindern.

Bei einer nächsten Weiterbildung wird die Berechtigungsprüfung bzw. werden die Berechtigungsprüfungen unter Verwendung von digitalen Schlüsseln durchgeführt, die von mindestens einer Zertifizierungsstelle erzeugt worden sind. Die Zertifizierungsstelle selbst ist Teil einer Zertifizierungskette. Das Verwenden von digitalen Schlüsseln bietet gegenüber dem Nutzen von Passwörtern eine erhöhte und beim zusätzlichen Verwenden von Passwörtern eine zusätzliche Sicherheit. Eine Zertifizierungs-Infrastruktur lässt sich beispielsweise gemäß Standard X.509 der ITU-T (International Telecommunication Union - Telecommunication Sector) aufbauen. Eingesetzt werden aber auch andere Infrastrukturen, z.B. eine Infrastruktur gemäß den Vorgaben der IETF (Internet Engineering Task Force) im Request for Comment 2459, Januar 1999. Das Aufbauen solcher Infrastrukturen und das Einbeziehen in das erfindungsgemäße Verfahren gewährleistet allen beteiligten Seiten eine hohe Sicherheit. Beispielsweise lassen sich ungültige Schlüssel auf einfache Art und Weise sperren.

Bei einer anderen Weiterbildung wird ein geheimzuhaltender digitaler Schlüssel für das Verschlüsseln eingesetzt. Der geheimzuhaltende Schlüssel wird in einer elektronisch gesicherten Speichereinheit gespeichert. Bei einer Ausgestaltung ist die gesicherte Speichereinheit Bestandteil einer sogenannten Chipkarte, die einen eingegossenen Prozessor und die gesicherte Speichereinheit enthält. Die gesicherte Speichereinheit lässt sich ausschließlich durch diesen Prozessor lesen und schreiben. Vor dem Zugriff wird bei einer Ausgestaltung eine Berechtigungsprüfung ausgeführt, die beispiels-

weise die Abfrage eines Passwortes oder einer Geheimnummer enthält. Vorzugsweise wird ein asymmetrisches Verschlüsselungsverfahren eingesetzt.

Bei einer anderen Weiterbildung des erfindungsgemäßen Verfahrens betrifft die Anforderung die Absicherung einer Zahlung. Die Absicherung der Zahlung ist das Kernstück der Diensterbringung über ein Datenübertragungsnetz und für die Akzeptanz dieser Verfahren daher besonders wichtig. So werden Anforderungen gestellt, mit denen durch einen Dritten die Haftung für den Fall übernommen wird, dass der Dienstnutzer den genutzten Dienst nicht zahlt. Diese Zusicherungen sind bei einer Ausgestaltung zeitlich begrenzt, beispielsweise auf einen Tag oder auf die Zeitdauer einer Verbindung zwischen Dienstnutzer und Diensterbringungsrechner.

Bei einer anderen Weiterbildung des erfindungsgemäßen Verfahrens stellt die Prüfeinheit zur Bearbeitung der Anforderung eine Anfrage zum Erhalt eines Zahlungszertifikats an einen Zertifizierungsrechner. Der Zertifizierungsrechner erzeugt ein digitales Zahlungszertifikat, das die Zahlung absichert. Das Zahlungszertifikat wird dann über die Prüfeinheit zum Diensterbringungsrechner weitergeleitet. Auch zum Erzeugen des digitalen Zahlungszertifikates werden bei einer Ausgestaltung Verschlüsselungs- und/oder Unterschriftsverfahren unter Verwendung von digitalen Schlüsseln eingesetzt. Auch der Zertifizierungsrechner ist bei einer Ausgestaltung Teil einer Zertifizierungsinfrastruktur. Die vom Zertifizierungsrechner ausgestellten Zertifikate haben eine kürzere Gültigkeitsdauer als die Zertifikate für die digitalen Schlüssel. Durch die kürze Gültigkeitsdauer lässt sich ein Missbrauch der Zahlungszertifikate bzw. Zahlungsattribute besser verhindern. Ein Zertifizierungsrechner ist bei einer Ausgestaltung ein sogenannter TrustedA-Rechner (Trusted Authorizer), wie er von der irischen Firma SSE verkauft wird, siehe www.sse.ie.

Bei einer alternativen Weiterbildung erzeugt die Prüfeinheit bei der Bearbeitung der Anforderung selbst ein Zahlungszertifikat, das die Zahlung absichert. In diesem Fall ist die Prüfeinheit beispielsweise im Besitz eines Bankinstitutes bzw. eines Kreditinstitutes. Das durch die Prüfeinheit erzeugte Zahlungszertifikat wird auch an den Diensterbringungsrechner weitergeleitet. Der Diensterbringungsrechner prüft dann beispielsweise das Zahlungszertifikat und veranlasst die Diensterbringung, falls das Zahlungszertifikat gültig ist und die Anforderung bestätigt.

Bei einer nächsten Weiterbildung erbringen die Diensterbringungsrechner die Funktionen elektronischer Kaufplattformen und/oder elektronischer Dienstleistungsplattformen, z.B.:

- Abruf von Musikdaten, Videodaten oder Programmdaten,
- e-Business, Bankgeschäfte, Handelgeschäfte,
- Informationsdienste,
- sichere digitale Sprachübertragung.

Damit bietet die Zugangsfunktion dem Dienstnutzer Zugang beispielsweise zu einer virtuellen Einkaufsmeile. Das erfindungsgemäße Verfahren wird jedoch auch für andere Dienste eingesetzt, bei denen zu sichernde Daten der Dienstnutzer in die Diensterbringung einbezogen werden, beispielsweise Kreditgeschäfte.

Die Erfindung betrifft außerdem ein Programm mit einer Befehlsfolge, bei deren Ausführung durch einen Prozessor das erfindungsgemäße Verfahren oder eine seiner Weiterbildung ausgeführt wird. Außerdem ist eine Datenverarbeitungsanlage geschützt, die ein solches Programm enthält. Für das Programm und die Datenverarbeitungsanlage gelten somit die oben genannten technischen Wirkungen.

Zum Verschlüsseln lassen sich asymmetrische Verschlüsselungsverfahren einsetzen, z.B. das RSA-Verfahren (Revist, Shamir, Adleman). Aber auch symmetrische Verfahren werden eingesetzt,

z.B. der dreifache DES-Algorithmus (Data Encryption Standard). Ein anderes gebräuchliches Verschlüsselungsverfahren ist beispielsweise das ECC-Verfahren (Elliptic Curve Cryptographie).

Im Folgenden werden Ausführungsbeispiele der Erfindung an Hand der beiliegenden Zeichnungen erläutert. Darin zeigen:

Figur 1 ein Datenübertragungsnetz und einen Zentralrechner,

Figur 2 Verfahrensschritte zur Erbringung des Dienstes "Buchkauf",

Figur 3 die Bearbeitung einer Zahlungsfähigkeitsanfrage, und

Figur 4 die Bearbeitung einer Attributanfrage.

Figur 1 zeigt ein Datenübertragungsnetz 10, das einen Zentralrechner 12 enthält. Bestandteil des Datenübertragungsnetzes 10 sind auch das Internet 14 sowie ein Mobilfunknetz 16. Im Internet 14 werden digitale Daten gemäß Protokoll TCP/IP (Transmission Control Protocol/Internet Protocol) übertragen. Im Mobilfunknetz 16 werden digitale Daten beispielsweise gemäß GSM-Standard (Global System for Mobile Communication) oder gemäß UMTS-Standard (Universal Mobile Telecommunication System) übertragen.

Über das Internet 14 oder das Mobilfunknetz 16 können eine Vielzahl von Dienstnutzern, beispielsweise mehrere Tausend, Verbindungen zwischen den von ihnen genutzten Endgeräten und dem Zentralrechner 12 aufbauen. In Figur 1 ist das Endgerät 18 eines Dienstnutzers A dargestellt. Das Endgerät 18 ist beispielsweise ein tragbarer Rechner oder ein Mobilfunkgerät und enthält eine Smartkarte 20.

Über das Internet 14 und das Mobilfunknetz 16 lassen sich außerdem Verbindungen zwischen einer Vielzahl von Diensterbringungsrechnern und dem Zentralrechner 12 aufbauen. Beispielsweise sind mehrere hundert Diensterbringungsrechner beim Zentralrechner 12 registriert. In Figur 1 sind zwei Diensterbringungsrechner 22 und 24 dargestellt, die Diensterbringern B und Z gehören. Weitere Diensterbringungsrechner 26 sind durch Punkte angedeutet. In den Diensterbringungsrechnern 22 und 24 sind jeweils voneinander verschiedene digitale Zertifikate ZB bzw. ZZ gespeichert.

Die Smartkarte 20, das Zertifikat ZB und das Zertifikat ZZ sind von einem PKI-Zentrum 28 (public key infrastructure) ausgegeben worden, nachdem die Identität des Dienstnutzers A, des Diensterbringers B bzw. des Diensterbringers Z durch eine lokale Ausgabestelle geprüft worden sind. Die lokale Ausgabestelle wird auch als LRA-Stelle (Local Registration Authority) bezeichnet. Die Ausgabe der Smartkarte 20 bzw. des Zertifikates ZB wird durch einen Pfeil 30 bzw. 32 verdeutlicht.

Wird die Smartkarte 20 oder ein Zertifikat ZB, ZZ gesperrt, so benachrichtigt das PKI-Zentrum 28 den Zentralrechner 12, siehe Pfeil 34. Der Zentralrechner 12 schließt dann die ungültige Smartkarte 20 bzw. die ungültigen Zertifikate ZB, ZZ bei Berechtigungsprüfungen von weiteren Transaktionen aus.

Der Zentralrechner 12 ist ein sehr leistungsstarker Rechner und enthält eine Zugangseinheit 36, eine Prüfeinheit 38 und eine Datenbank 40. Die Zugangseinheit 36 stellt eine Zugangsmöglichkeit für die Dienstnutzungsrechner 18 dar und ist mit dem Internet 14 und dem Mobilfunknetz 16 verbunden. Außerdem lassen sich über die Zugangseinheit 36 die Verbindungen zwischen dem Zentralrechner 12 und den Diensterbringungsrechnern 22 bis 26 aufbauen, siehe Verbindungen 42 und 44. Die Zugangseinheit 36 führt auch Berechtigungsprüfungen durch, die unten an Hand der Figur 2 näher erläutert werden.

Die Prüfeinheit 38 prüft, ob für einen Dienstnutzer die Gewähr übernommen werden kann, dass er zahlungsfähig ist. Dazu wird ein sogenanntes Zahlungsattribut erzeugt. Die dabei ausgeführten Verfahrensschritte werden unten an Hand der Figuren 3 und 4 näher erläutert.

Die Zugangseinheit 36 und die Prüfeinheit 38 haben Zugriff auf die Datenbank 40. In der Datenbank 40 sind Dienstnutzerprofile 46 und Dienst-Nutzerdaten 48 gespeichert. Die Datenbank 40 wird mit einem kommerziell verfügbaren Verzeichnisverwaltungsprogramm verwaltet, z.B. mit dem Programm DIRX der Firma SIEMENS AG. Die Dienstnutzerprofile 46 enthalten Daten über die Gewohnheiten der Dienstnutzer bei der Auswahl der Diensterbringungsrechner 22 bis 24. Außerdem enthalten die Dienstnutzerprofile 46 beispielsweise Angaben über einen Kreditrahmen, bis zu dem der Betreiber des Zentralrechners die Gewähr für die Zahlungsfähigkeit der Dienstnutzer übernimmt. Die Dienst-Nutzerdaten 48 gehören, abhängig vom betroffenen Dienst, dem Erbringer dieses Dienstes. Beispielsweise enthalten Dienst-Nutzerdaten 48 für den Dienst "Buchverkauf", der durch den Diensterbringungsrechner 22 erbracht wird, die folgenden Angaben:

- die bereits durch einen Dienstnutzer bestellten Bücher,
- ein Kennzeichen für den Dienstnutzer, und
- Angaben über vom Dienstnutzer noch nicht beglichene Rechnungen im Zusammenhang mit den Buchkäufen.

Die Dienstnutzerprofile 46 sind mit einem sogenannten öffentlichen Schlüssel S1-E (Encryption) verschlüsselt. Beim Lesen der Dienstnutzerprofile 46 aus der Datenbank 40 werden die Daten mit Hilfe eines geheimgehaltenen privaten Schlüssels S1-D (Decryption) entschlüsselt. Die beiden Schlüssel S1-E und S1-D sind Partnerschlüssel eines asymmetrischen Verschlüsselungsverfahrens. Der private Schlüssel S1-D lässt sich durch konstruktive und/oder elektronische Maßnahmen im Zentralrechner 12 geheimhalten.

Die Dienst-Nutzerdaten 48 werden in den Diensterbringungsrechnern 22 bis 26 mit voneinander verschiedenen öffentlichen Schlüsseln der einzelnen Diensterbringer verschlüsselt, siehe beispielsweise die öffentlichen Schlüssel S2-E bzw. S3-E im Diensterbringungsrechner 22 bzw. 24. Anschließend werden die verschlüsselten Dienst-Dienstnutzerdaten über die Verbindung 42 bzw. 44 übertragen und in der Datenbank 40 verschlüsselt gespeichert. Andererseits lassen sich die Dienst-Nutzerdaten 48 auch verschlüsselt aus der Datenbank 40 lesen, verschlüsselt über die Verbindung 42 bzw. 44 zu einem Diensterbringungsrechner 22 bzw. 24 übertragen und dort mit Hilfe eines Partnerschlüssels S2-D bzw. S3-D entschlüsseln.

Figur 2 zeigt Verfahrensschritte zur Erbringung des Dienstes "Buchkauf" durch den Diensterbringungsrechner 22. Will der Dienstnutzer A ein Buch kaufen, so baut er eine Verbindung zwischen seinem Dienstnutzungsrechner 18 und dem Zentralrechner 12 auf, genauer gesagt mit der Zugangseinheit 36 des Zentralrechners 12. Zwischen Dienstnutzungsrechner 18 und Zugangseinheit 36 wird ein Authentisierungsverfahren 60 ausgeführt, bei dem ein Nutzerkennzeichen des Dienstnutzers A durch die Zugangseinheit 36 erfragt wird. An Hand des Nutzerkennzeichens wird ein öffentlicher Schlüssel S4-E ermittelt, welcher der Partnerschlüssel zu dem in der Smartkarte 20 gespeicherten Schlüssel S4-D des Dienstnutzers A ist. Unter Verwendung des öffentlichen Schlüssels S1-E des Zentralrechners 12 werden die vom Dienstnutzungsrechner 18 kommenden Daten verschlüsselt. Die Zugangseinheit 36 entschlüsselt diese Daten mit Hilfe des privaten Schlüssels S1-D. Die von der Zugangseinheit 36 zum Dienstnutzungsrechner 18 zu übertragenden Daten werden andererseits in der Zugangseinheit 36 mit Hilfe des öffentlichen Schlüssels S4-E verschlüsselt und anschließend über das Internet 14 zum Dienstnutzungsrechner 18 übertragen. Im Dienstnutzungsrechner 18 wird zum Entschlüsseln der von der Zugangseinheit 36 kommenden Daten ein privater Schlüssel S4-D benutzt, der in der Smartkarte 20 gesichert gespeichert ist. Vor der Benutzung des öffentlichen

Schlüssels S4-E prüft die Zugangseinheit 36, ob dieser Schlüssel noch gültig ist.

Anschließend fordert die Zugangseinheit 36 ein Dienstnutzerprofil NP-A des Dienstnutzers A von der Datenbank 40 an, siehe Pfeil 62. An Hand der im Dienstnutzerprofil NP-A gespeicherten Daten erstellt die Zugangseinheit 36 dem Dienstnutzer A eine Auswahlliste mit Adressen von Diensterbringungsrechnern, die er häufig anwählt. In dieser Liste ist auch die Internetadresse des Diensterbringungsrechners 22 vermerkt.

Der Dienstnutzer A wählt aus der Liste einen Diensterbringungsrechner aus, beispielsweise den Diensterbringungsrechner 22, siehe Pfeil 64. In einem nächsten Verfahrensschritt 66 wird zwischen dem Dienstnutzungsrechner 18 und dem Diensterbringungsrechner 22 ein gesicherter Übertragungskanal aufgebaut. Der Diensterbringungsrechner 22 übermittelt an den Dienstnutzungsrechner 18 seinen öffentlichen Schlüssel S2-E und ein Zertifikat ZB zu seinem öffentlichen Schlüssel S2-E. Im Dienstnutzungsrechner 18 wird das Zertifikat zu dem öffentlichen Schlüssel S2-E überprüft. Es sei angenommen, dass das Zertifikat ZB echt ist.

Der Dienstnutzer A verschlüsselt die von ihm zu sendenden Daten mit Hilfe des öffentlichen Schlüssels S2-E. Außerdem übermittelt der Dienstnutzungsrechner 18 seinen öffentlichen Schlüssel S4-E und einen Verweis auf ein Zertifikat zu seinem öffentlichen Schlüssel S4-E, beispielsweise einen Verweis auf das PKI-Zentrum 28 oder einen Verweis auf den Zentralrechner 12. Der Diensterbringungsrechner 22 überprüft das Zertifikat unter Verwendung mindestens eines öffentlichen Schlüssels, dem er vertraut. Das Zertifikat sei echt. Vom Diensterbringungsrechner 22 kommende Daten werden deshalb mit Hilfe des öffentlichen Schlüssels S4-E verschlüsselt.

Um sogenannte Replay-Angriffe und sogenannte Man-in-the-Middle-Angriffe auszuschließen, wird beim Aufbau des gesicherten Übertragungskanals 66 auch ein sogenanntes Challenge-Response-Verfahren eingesetzt, bei dem Zufallszahlen zwischen dem Dienstnutzungsrechner 18 und dem Diensterbringungsrechner 22 ausgetauscht werden, die sich bei jedem Verbindungsaufbau ändern.

Der Dienstnutzer A wählt über den gesicherten Übertragungskanal ein Buch aus und bekundet durch Betätigen einer Schaltfläche sein Kaufinteresse. Danach wird zwischen dem Diensterbringungsrechner 22 und dem Zentralrechner 12 eine Verbindung aufgebaut, genauer gesagt zwischen dem Diensterbringungsrechner 22 und der Zugangseinheit 36 des Zentralrechners 12.

In einem Verfahrensschritt 68 wird die Berechtigung des Diensterbringungsrechners 22 geprüft. Für diese Prüfung übermittelt der Diensterbringungsrechner 22 ein Zertifikat ZB zu seinem öffentlichen Schlüssel S2-E an die Zugangseinheit 36. Die Zugangseinheit 36 überprüft dieses Zertifikat ZB.

Die vom Diensterbringungsrechner 22 kommenden Daten sind mit Hilfe des öffentlichen Schlüssels S1-E des Zentralrechners 12 verschlüsselt. Der Zentralrechner 12 kann diese Daten unter Verwendung seines privaten Schlüssels S1-D entschlüsseln.

Auch der Zentralrechner 12 sendet ein Zertifikat zu seinem öffentlichen Schlüssel S1-E an den Diensterbringungsrechner 22. Vor der Verwendung des Schlüssels S1-E prüft der Diensterbringungsrechner 22 das Zertifikat zu dem öffentlichen Schlüssel S1-E.

Der Diensterbringungsrechner 22 fordert nun Kundendaten KD-A des Dienstnutzers A vom Zentralrechner 12 an. In einem Verfahrensschritt 70 werden die Kundendaten KD-A aus der Datenbank 40 ausgelesen und an den Diensterbringungsrechner 22

übertragen. Die Kundendaten KD-A sind dabei mindestens einmal verschlüsselt, und zwar mit dem öffentlichen Schlüssel S2-D.

Aufgrund der Kundendaten KD-A erstellt der Diensterbringungsrechner 22 automatisch einen Kaufvertrag. Die Vertragsdaten werden vom Dienstnutzungsrechner 18 nach der Eingabe einer PIN (Personal Identity Number), einer TAN (Transaction Number) oder eines biometrischen Merkmals unter Verwendung des privaten Schlüssels S4-D unterzeichnet. Auch der Diensterbringungsrechner 22 des Diensterbringers B unterzeichnet die Vertragsdaten mit seinem privaten Schlüssel S2-D. Die unterzeichneten Daten werden zwischen dem Dienstnutzungsrechner 18 und dem Diensterbringungsrechner 22 über den gesicherten Übertragungskanal ausgetauscht.

Im Diensterbringungsrechner 22 wird die Unterschrift des Dienstnutzungsrechners 18 geprüft. Dazu lässt sich der öffentliche Schlüssel S4-E nutzen. Es sei angenommen, dass die Unterschrift echt ist. Der Dienstnutzungsrechner 18 prüft die Unterschrift des Diensterbringungsrechners 22 unter Verwendung des öffentlichen Schlüssels S2-E.

In einem Verfahrensschritt 74 stellt der Diensterbringungsrechner 22 eine Anfrage zur Zahlungsabwicklung mit dem Dienstnutzer A und gibt dabei den Betrag an, für den der Dienstnutzer A bei ihm Bücher gekauft hat, beispielsweise DM 300. Die Anfrage und der Betrag werden mit Hilfe des privaten Schlüssels S2-D einer Unterschrift SignB unterschrieben.

Die Prüfeinheit 38 überprüft die Unterschrift SignB mit Hilfe des öffentlichen Schlüssels S2-E. Es sei angenommen, dass die Unterschrift echt ist. Die Prüfeinheit 38 prüft mit Hilfe eines unten an Hand der Figur 3 näher erläuterten Verfahrens, ob ein Kreditinstitut eine Deckungszusage übernimmt, ob der Betrag im Rahmen einer Kreditvereinbarung mit einem Kreditinstitut liegt oder ob der Dienstnutzer A seine Erlaubnis zur sofortigen Abbuchung von seinem Konto gegeben hat. Es sei

angenommen, dass eine Erlaubnis zur sofortigen Abbuchung vorliegt. Deshalb beschafft die Prüfungseinheit 38 nun nach einem unten an Hand der Figur 4 erläuterten Verfahren ein Zahlungsattribut. Die Prüfeinheit 38 bucht dann den Betrag von DM 300 vom Konto des Dienstnutzers A ab und überweist den Betrag auf ein Treuhandkonto, um ihn später an den Betreiber des Diensterbringungsrechners B zu überweisen.

In einem Verfahrensschritt 76 wird zum Diensterbringungsrechner 22 ein Zahlungsattribut übertragen, in dem bestätigt wird, dass der Dienstnutzer A den Betrag von DM 300 bezahlt bzw. bezahlt hat. Das Zahlungsattribut wird mit Hilfe des privaten Schlüssels S1-D des Zentralrechners 12 unterschrieben und zum Diensterbringungsrechner 22 übermittelt, gegebenenfalls auch in verschlüsselter Form.

In einem Verfahrensschritt 78 bestätigt der Diensterbringungsrechner 22 dem Dienstnutzungsrechner 18, dass der Auftrag angenommen und die Auslieferung der Bücher veranlasst worden ist. Zur Übertragung der Auftragungsbestätigung wird der gesicherte Übertragungskanal zwischen dem Diensterbringungsrechner 22 und dem Dienstnutzungsrechner 18 genutzt.

In einem Verfahrensschritt 80 archiviert der Diensterbringungsrechner 22 die den Kaufvertrag betreffenden Daten in der Datenbank 40, gegebenenfalls verschlüsselt.

Nachfolgende weitere Verfahrensschritte 82 sind durch Punkte angedeutet. Der Diensterbringungsrechner 22 veranlasst über ein Logistiksystem die Auslieferung des Buches an den Dienstnutzer A. Bei der Übergabe des Buches bestätigt der Dienstnutzer A den Erhalt. Die Bestätigung wird beispielsweise über das Mobilfunknetz 16 mit Hilfe einer SMS-Nachricht (Short Message Service) an den Zentralrechner 12 übertragen und dort für spätere Nachweiszwecke gespeichert. Gleichzeitig wird die Überweisung des Betrages von DM 300 von dem Treuhandkonto auf ein Konto des Diensterbringers B überwiesen.

Figur 3 zeigt die Bearbeitung der Zahlungsfähigkeitsanfrage. Die Zahlungsfähigkeitsanfrage wird von der Prüfeinheit 38 an einen Bankrechner 100 gestellt, der einem Kreditinstitut oder einer Bank gehört. Die Zahlungsfähigkeitsanfrage wird durch einen Pfeil 102 dargestellt und enthält Angaben zum Dienstnutzer A sowie Angaben zum Betrag. Der Bankrechner 100 überprüft, ob eine Deckungszusage erteilt werden kann. Im Ausführungsbeispiel ist dies der Fall und mit Hilfe einer Auskunft 104 teilt der Bankrechner 100 der Prüfeinheit 38 mit, dass der Dienstnutzer A die Erlaubnis erteilt hat, von seinem Konto sofort abzubuchen. Bei einem anderen Ausführungsbeispiel teilt der Bankrechner 100 beispielsweise mit, dass der Dienstnutzer einen Kreditrahmen von zehn tausend D-Mark hat.

Für die Übertragung der Zahlungsfähigkeitsanfrage 102 und die Übertragung der Auskunft 104 lassen sich ebenfalls digitale Schlüssel einer Infrastruktur und zugehörige Zertifikate nutzen, um einem Missbrauch vorzubeugen. Bei einem Ausführungsbeispiel werden die zwischen der Prüfeinheit 38 und dem Bankrechner 100 ausgetauschten Daten nach einem digitalen Verschlüsselungsverfahren verschlüsselt.

Die Auskunft 104 des Bankrechners 100 wird in dem Dienstnutzerprofil 46 gespeichert. Die Auskunft ist vertraulich und wird dem Diensterbringungsrechner 22 nicht zur Verfügung gestellt.

Figur 4 zeigt die Bearbeitung einer Zahlungsattributanfrage 122, die nach dem Erhalt der Auskunft 104 von der Prüfeinheit 38 an einen Zahlungsattribut-Server 120 gerichtet wird, der auch als TrustedA-Rechner bezeichnet wird. Beispielsweise wird ein TrustedA-Rechner der Firma SSE eingesetzt, siehe www.sse.ie.

Die Zahlungsattributanfrage 122 enthält u.a. die folgenden Daten:

- den Betrag von DM 300,
- den Namen der Prüfeinheit 38, die das Zahlungsattribut beantragt, und
- den Namen des Diensterbringungsrechners 22, für den das Zahlungsattribut bestimmt ist.

Der Zahlungsattribut-Server 120 stellt ein Zahlungsattribut 124 aus, mit dem folgende Daten zertifiziert, d.h. mit einer digitalen Unterschrift SignAS des Attribut-Servers versehen, werden:
- der Betrag von DM 300,
- den Namen der Prüfeinheit 38, die das Zahlungsattribut 124 beantragt,
- den Namen des Diensterbringungsrechners 22, für den das Zahlungsattribut 124 bestimmt ist, und
- ein Ablaufdatum.

Das Zahlungsattribut wird in einem Verfahrensschritt 124 vom Attribut-Server 120 zur Prüfeinheit 38 übermittelt. Die Prüfeinheit prüft die Angaben und die Unterschrift SignAS mit Hilfe mindestens eines öffentlichen Schlüssels, der als vertrauensvoll eingestuft ist.

Auch der Diensterbringungsrechner 22 prüft bei einem Ausführungsbeispiel die Echtheit des Zahlungsattributes 124. Der Kauf wird nur bestätigt, wenn das Zahlungsattribut echt ist.

Die an Hand der Figuren 1 bis 34 erläuterten Einheiten lassen sich mit Hilfe von Programmen realisieren. Eingesetzt werden aber auch Schaltungseinheiten ohne einen Prozessor. Die Funktionen des Zentralrechners 12 lassen sich auch auf mehrere Rechner aufteilen, die an verschiedenen Stellen des Datenübertragungsnetzes 10 liegen.

Bei einem anderen Ausführungsbeispiel werden unterschiedliche Schlüssel zum Verschlüsseln der Daten zwischen dem Zentralrechner 12 und dem Diensterbringungsrechner einerseits und

zum Verschlüsseln der in der Datenbank 40 zu speichernden Dienst-Dienstnutzerdaten 48 verwendet. Durch eine Doppelverschlüsselung der Übertragung auf den Verbindungen 42 und 44 lässt sich die Sicherheit weiter erhöhen.

Durch den Betreiber des Zentralrechners 12 werden die Diensterbringer vor der Erteilung einer Zugangsberechtigung auf ihre Vertrauenswürdigkeit hin überprüft. Auch neue Dienstnutzer werden auf ihre Vertrauenswürdigkeit hin überprüft. Durch diese Vorgehensweise lässt sich die Akzeptanz der erläuterten Verfahren sowohl auf der Seite der Diensterbringer als auch auf der Seite der Dienstnutzer weiter erhöhen.

Bei einem weiteren Ausführungsbeispiel werden die Funktionen des TrustedA-Rechners 120 durch den Zentralrechner 12 erbracht. Wird der Zentralrechner 12 bei einem nächsten Ausführungsbeispiel von einer Bank betrieben, so lassen sich auch die Funktionen des Bankrechners 100 durch den Zentralrechner 12 erbringen.

Die Funktionen des Zentralrechners 12 werden bei einem anderen Ausführungsbeispielen von mehreren Rechnern erbracht, die über das Internet 14 oder über Standleitungen miteinander verbunden werden.

Patentansprüche

1. Verfahren zum Erbringen von Diensten in einem Datenübertragungsnetz (10),

bei dem eine Zugangsfunktion (36) für mehrere Dienstnutzungsrechner (18) abhängig von Anforderungen von der Seite eines Dienstnutzungsrechners (18) eine Verbindung zwischen dem Dienstnutzungsrechner (18) und einem von mehreren durch einen Dienstnutzer (A) auswählbaren Diensterbringungsrechner (22 bis 26) ermöglicht,

bei dem in einer zentralen Datenbank (40) für die verschiedenen Dienstnutzer (A) zu sichernde Nutzerdaten (46) gespeichert werden, die zur Erbringung der Dienste verschiedener Diensterbringungsrechner (22 bis 26) erforderlich sind,

bei dem nach der Verbindungsaufnahme zwischen einem Dienstnutzungsrechner (18) und einem ausgewählten Diensterbringungsrechner (22) im Rahmen der Diensterbringung für den den Dienstnutzungsrechner (18) nutzenden Dienstnutzer (A) an eine von mehreren Diensterbringungsrechner (22 bis 26) genutzte Prüfeinheit (38) eine Anforderung gestellt wird, die nur unter Verwendung der zu sichernden Nutzerdaten (46) des Dienstnutzers (A) bearbeitet werden kann,

bei dem die Prüfeinheit (38) die Anforderung (74) unter Zugriff auf die zu sichernden Nutzerdaten (46) des Dienstnutzers (A) bearbeitet und das Bearbeitungsergebnis (76) an den die Anforderung (74) stellenden Diensterbringungsrechner (22) übermittelt,

und bei dem der Diensterbringungsrechner (22) seinen Dienst abhängig vom Bearbeitungsergebnis (76) erbringt.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Diensterbringungsrechner (22 bis 26) verschiedenen Betreibern gehören,

dass nach der Anwahl eines Diensterbringungsrechners dessen Berechtigung zum Stellen einer Anforderung mit Hilfe eines Berechtigungsprüfverfahrens (68, 74) geprüft wird,

und dass bei bestehender Berechtigung das Bearbeitungsergebnis (76) und bei fehlender Berechtigung kein Bearbeitungsergebnis (76) übermittelt wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die zu sichernden Nutzerdaten (46) verschlüsselt gespeichert werden,

und dass die Diensterbringungsrechner (22 bis 24) keinen Zugang zu einem zum Entschlüsseln der zu sichernden Nutzerdaten (46) erforderlichen digitalen Schlüssel (S1-D) haben.

4. Verfahren zum Erbringen von Diensten in einem Datenübertragungsnetz (10), insbesondere nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass in einer Datenbank (40) Dienst-Nutzerdaten (48) gespeichert sind, die dienstbezogene Daten für die Dienstnutzer (A) einzelner Diensterbringungsrechner (22 bis 26) enthalten,

dass nach der Auswahl eines Diensterbringungsrechners (22 bis 26) dessen Berechtigung zum Empfangen von Dienst-Nutzerdaten (48) betreffend den durch ihn erbrachten Dienst geprüft wird,

dass an den ausgewählten Diensterbringungsrechner (22) bei bestehender Berechtigung die Dienst-Nutzerdaten (48) desjenigen Dienstnutzers (A) übermittelt werden, der den ausgewählten Diensterbringungsrechner (22) ausgewählt hat,

und dass der Diensterbringungsrechner (22) seinen Dienst unter Verwendung der übermittelten Dienst-Nutzerdaten (48) erbringt.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass die Dienst-Nutzerdaten (48) verschlüsselt gespeichert und übertragen werden,

und dass verschiedene Diensterbringungsrechner (22, 24) verschiedene digitale Schlüssel (S2-D, S3-D) zum Entschlüsseln der Dienst-Nutzerdaten (48) verwenden.

6. Verfahren nach Anspruch 4 oder 5, dadurch gekennzeichnet, dass die Dienst-Nutzerdaten (48) mit einem zentralen Verschlüsselungsverfahren verschlüsselt sind,

und dass zum Verschlüsseln gemäß zentralem Verschlüsselungsverfahren ein für die Dienst-Dienstnutzerdaten verschiedener Diensterbringungsrechner (22 bi 26) gleicher digitaler Schlüssel verwendet wird.

7. Verfahren nach einem der Ansprüche 4 bis 6, dadurch gekennzeichnet, dass in einer von mehreren Diensterbringungsrechnern (22 bis 26) genutzten Datenbank (40) digitale Daten über Zahlungsvorgänge für verschiedene Diensterbringungsrechner (22 bis 26) gespeichert werden (80).

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Berechtigung des Dienstnutzers (A) unter Verwendung eines Berechtigungsprüfverfahrens (60) geprüft wird,

und dass die Auswahl nur beim Vorliegen einer Berechtigung zugelassen wird.

9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Berechtigungs-

prüfung unter Verwendung von digitalen Schlüsseln durchgeführt wird, die von mindestens einer Zertifizierungsstelle (28) erzeugt worden sind,

und dass die Zertifizierungsstelle (28) Teil einer Zertifizierungs-Infrastruktur ist.

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, dass ein geheimzuhaltender digitaler Schlüssel (S4-D) für das Verschlüsseln eingesetzt wird,

und dass der geheimzuhaltende digitale Schlüssel (S4-D) in einer elektronisch gesicherten Speichereinheit (20) gespeichert ist.

11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass die gesicherte Speichereinheit (20) Bestandteil einer Chipkarte (20) mit einem Prozessor ist,

und dass auf die gesicherte Speichereinheit (20) nach einer Berechtigungsprüfung nur mit dem Prozessor zugegriffen werden kann.

12. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennnzeichnet, dass die Anforderung (74) die Absicherung einer Zahlung betrifft.

13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass die Prüfeinheit (38) zur Bearbeitung der Anforderung eine Anfrage (102) zum Erhalt eines Zahlungszertifikats (104) an einen Zertifizierungsrechner (120) stellt,

und dass der Zertifizierungsrechner (120) ein digitales Zahlungszertifikat (124) erzeugt, das die Zahlung absichert,

und dass das Zahlungszertifikat über die Prüfeinheit (38) zum Diensterbringungsrechner (22) weitergeleitet wird.

14. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass die Prüfeinheit (38) bei der Bearbeitung der Anforderung (74) ein Zahlungszertifikat erzeugt, das die Zahlung absichert,

und dass das Zahlungszertifikat an den Diensterbringungsrechner (22) weitergeleitet wird.

15. Verfahren nach Anspruch 13 oder 14, dadurch gekennzeichnet, dass das Zahlungszertifikat (124) mit Hilfe eines digitalen Schlüssels erzeugt wird.

16. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Diensterbringungsrechner (22 bis 26) die Funktion elektronischer Kaufplattformen für verschiedene Produkte oder Produktgruppen erbringen und/oder elektronischer Dienstleistungsplattformen für verschiedene Dienstleistungen oder Dienstleistungsgruppen.

17. Programm mit einer Befehlsfolge, bei deren Ausführung durch einen Prozessor die Verfahrensschritte nach einem der vorhergehenden Ansprüche ausgeführt werden.

18. Datenverarbeitungsanlage (12), gekennzeichnet durch ein Programm nach Anspruch 17.

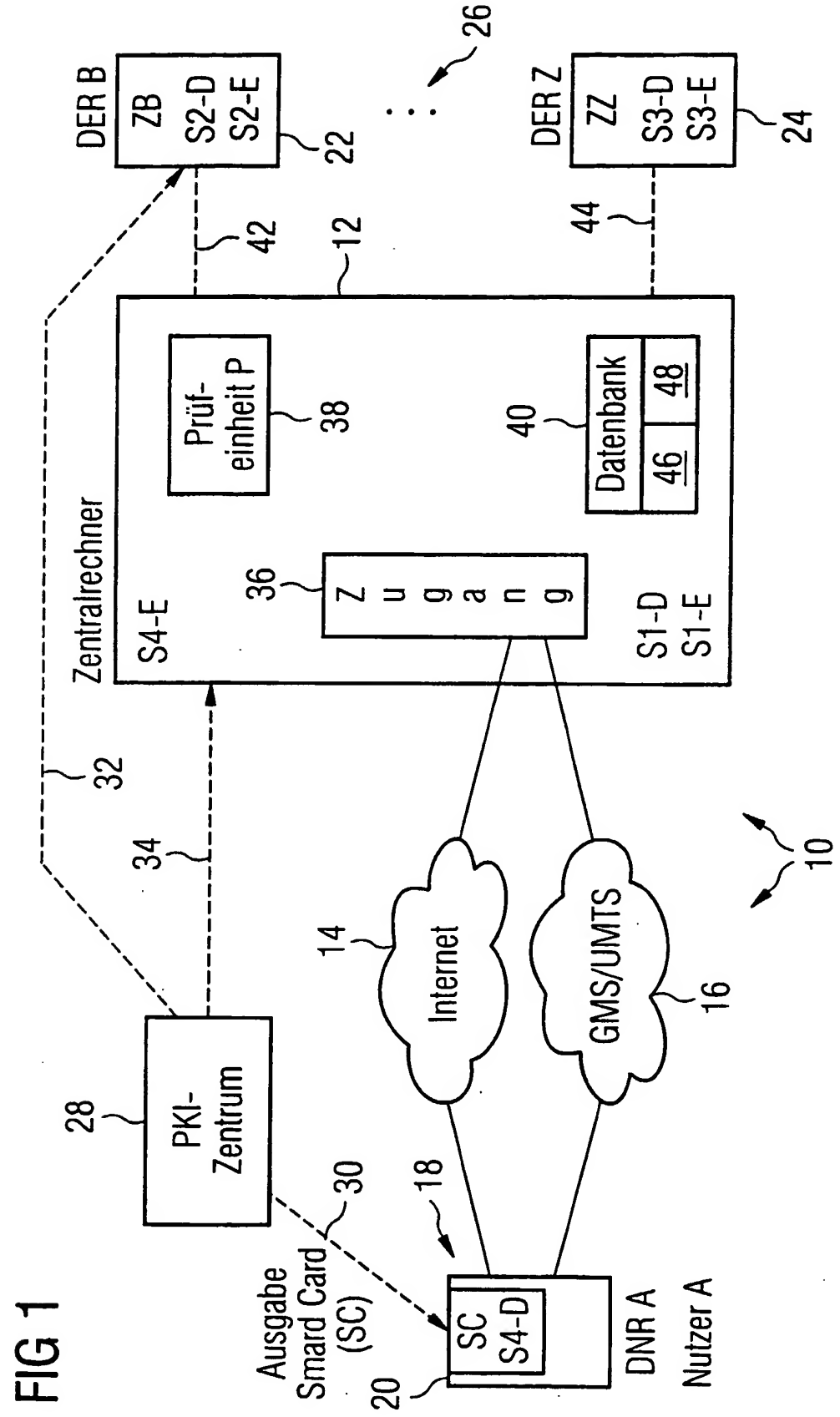

DER B
ZB
S2-D
S2-E
22
26
DER Z
ZZ
S3-D
S3-E
24
42
12
44
Zentralrechner
S4-E
Prüf-
einheit P
38
40
Datenbank
46
48
36
Z u g a n g
S1-D
S1-E
32
34
14
Internet
GMS/UMTS
16
10
28
PKI-
Zentrum
30
18
Ausgabe
Smard Card
(SC)
SC
S4-D
20
DNR A
Nutzer A

FIG 1

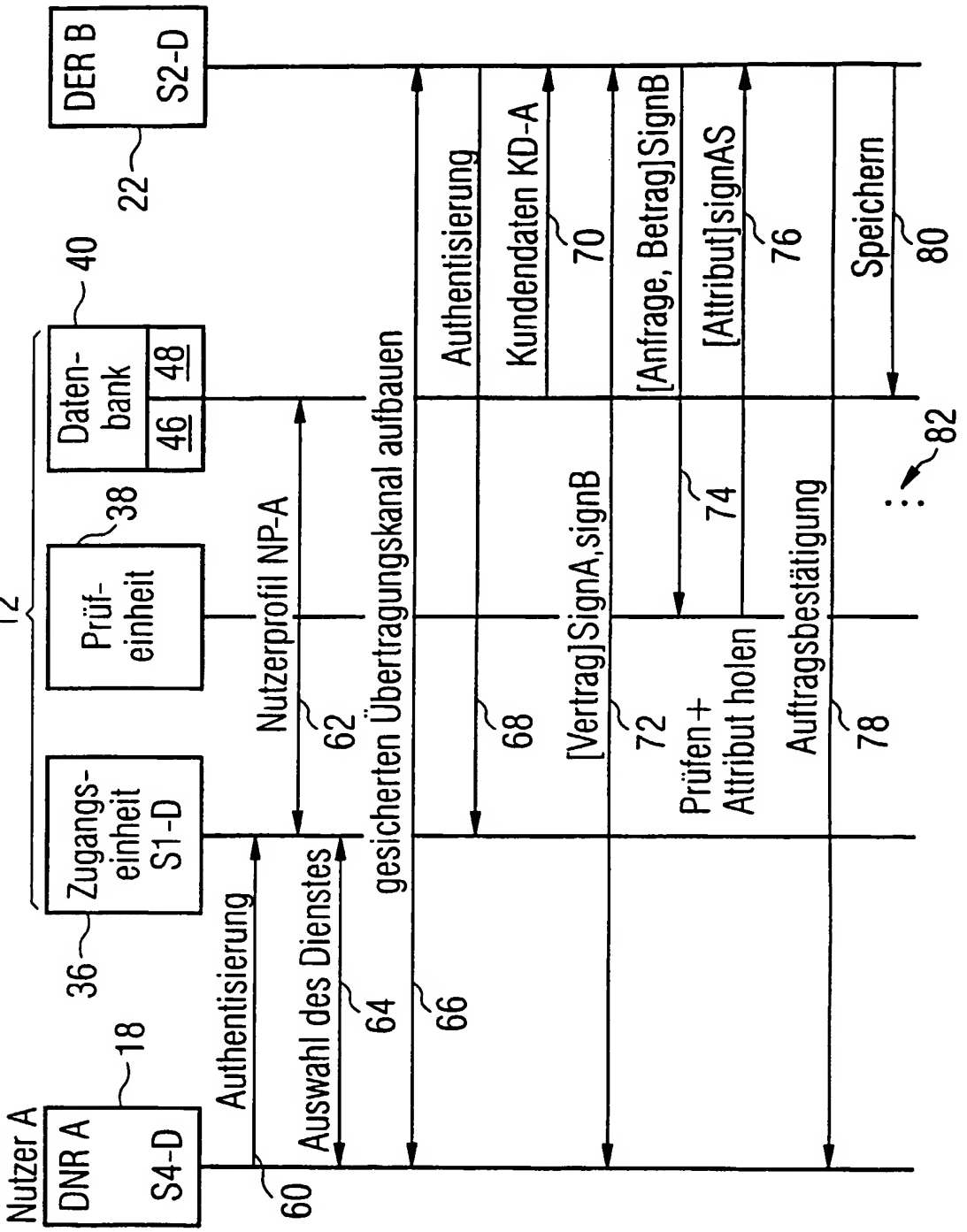

Nutzer A
DNR A
S4-D
18
Zugangs-
einheit
S1-D
36
12
Prüf-
einheit
38
Daten-
bank
46
48
40
DER B
S2-D
22
Authentisierung
60
Auswahl des Dienstes
64
gesicherten Übertragungskanal aufbauen
66
Nutzerprofil NP-A
62
Authentisierung
68
Kundendaten KD-A
70
[VertragJSignA,signB
72
[Anfrage, BetragJSignB
74
Prüfen +
Attribut holen
[AttributJsignAS
76
Auftragsbestätigung
78
Speichern
80
82

FIG 2

FIG 3

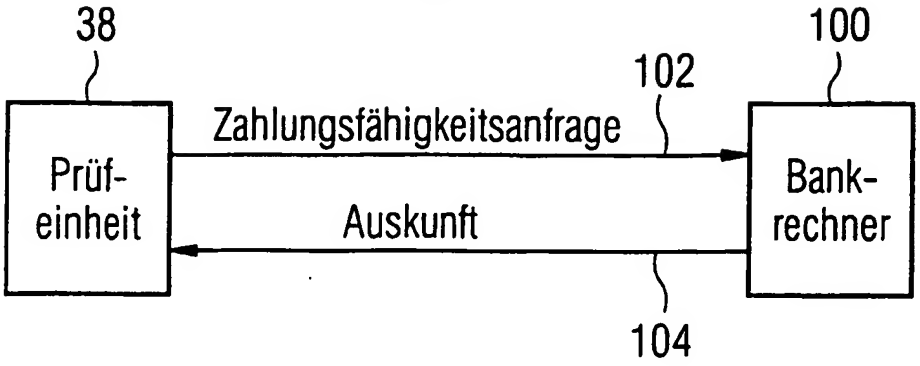
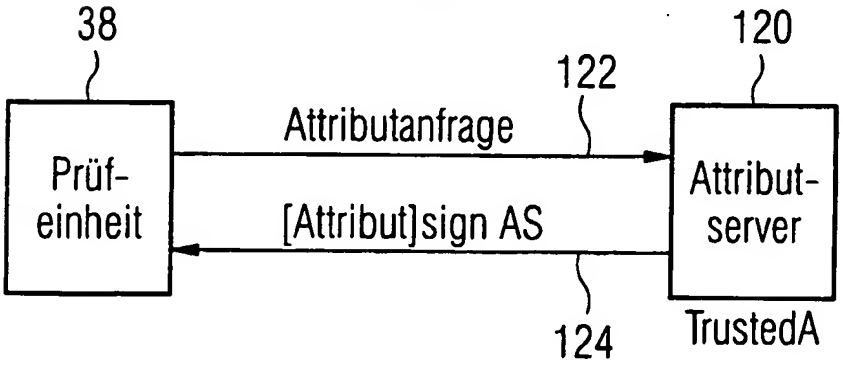

38
100
102
Zahlungsfähigkeitsanfrage
Prüf-
einheit
Auskunft
Bank-
rechner
104

FIG 4


38
120
122
Attributanfrage
Prüf-
einheit
[Attribut]sign AS
Attribut-
server
124
TrustedA